



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001265636 A**(43) Date of publication of application: **28.09.01**

(51) Int. Cl.

**G06F 12/00****G06F 12/14****G06F 15/00****G06F 17/30**(21) Application number: **2000072354**(71) Applicant: **CANON INC**(22) Date of filing: **15.03.00**(72) Inventor: **KIYONO HIROYUKI**

(54) **DOCUMENT MANAGEMENT UNIT, DOCUMENT MANAGEMENT METHOD AND STORAGE MEDIUM**

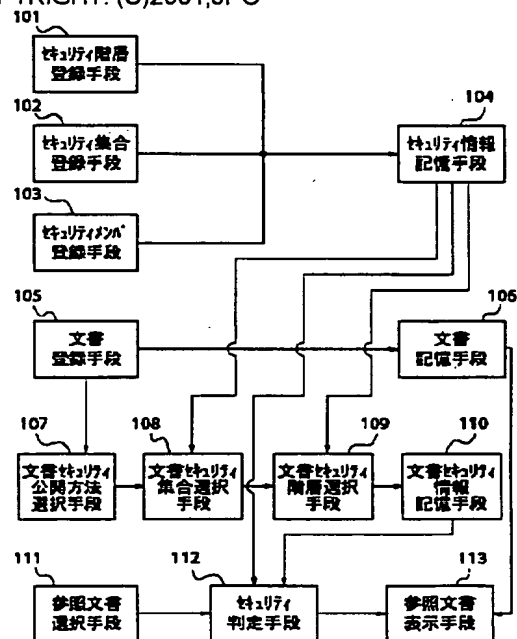
selection means 109.

COPYRIGHT: (C)2001,JPO

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a document management unit for easily setting and managing security for documents.

**SOLUTION:** In this document management unit, document data specified by a user are registered to a document storage means 106 by a document registration means 105 and a document security publicizing method selection means 107 is requested to select the publicizing method of the document. The document security publicizing method selection means 107 performs a processing for making the user select the method for publicizing the document data. Then, the processing for selecting a security set to be added to the document data from a security information storage means 104 is performed by a document security set selection means 108, and the processing for selecting a security hierarchy to be added to the document data to be registered from the security information storage means 104 is performed by a document security hierarchy



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2001-265636  
(P2001-265636A)

(43)公開日 平成13年9月28日(2001.9.28)

(51)IntCl. <sup>7</sup>	識別記号	F I	テ-マ-コ-ト (参考)	
G 0 6 F	12/00	5 3 7	5 3 7 A	5 B 0 1 7
	12/14	3 1 0	3 1 0 K	5 B 0 7 5
	15/00	3 3 0	3 3 0 A	5 B 0 8 2
	17/30	1 1 0	1 1 0 F	5 B 0 8 5
		1 2 0	1 2 0 B	
審査請求 未請求 請求項の数18 O L (全 15 頁)				

(21)出願番号 特願2000-72354(P2000-72354)

(22)出願日 平成12年3月15日(2000.3.15)

(71)出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72)発明者 清野 博之

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74)代理人 100081880

弁理士 渡部 敏彦

Fターム(参考) 5B017 AAD1 BA06 BB02 CAD7 CA08  
CA16

5B075 KK07 KK43 KK54 KK63

5B082 AA11 EA10 GA13 GC03

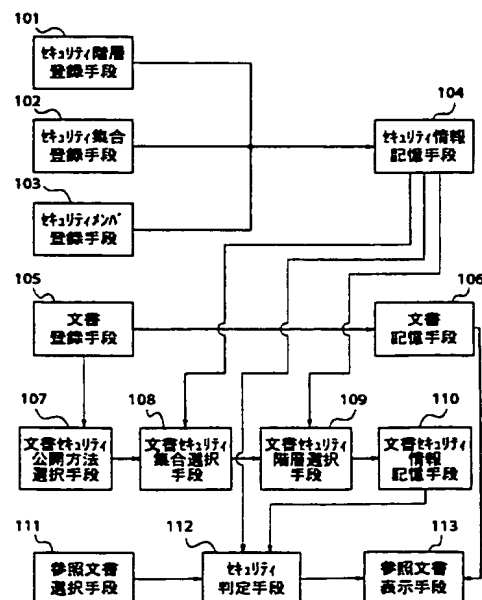
5B085 AED3 AEO6

(54)【発明の名称】 文書管理装置、文書管理方法および記憶媒体

(57)【要約】

【課題】 文書に対するセキュリティの設定および管理を容易に行うことができる文書管理装置を提供する。

【解決手段】 文書管理装置においては、文書登録手段105により、ユーザにより指定された文書データを文書記憶手段106に登録するとともに、文書セキュリティ公開方法選択手段107に対して文書の公開方法を選択することを要求する。文書セキュリティ公開方法選択手段107は、文書データの公開方法をユーザに選択させるための処理を行う。そして、文書セキュリティ集合選択手段108によりセキュリティ情報記憶手段104の中から文書データに付加するセキュリティ集合を選択するための処理を行い、文書セキュリティ階層選択手段109によりセキュリティ情報記憶手段104の中から登録する文書データに対して付加するセキュリティ階層を選択するための処理を行う。



## 【特許請求の範囲】

【請求項1】 文書格納手段に格納された文書を公開可能に管理する文書管理装置において、前記文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録するセキュリティ情報登録手段と、前記登録されたセキュリティ情報の中から前記文書に付加するセキュリティ情報を選択するセキュリティ情報選択手段と、前記選択したセキュリティ情報を前記文書に対応付けて付加するセキュリティ情報付加手段と、前記文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する閲覧要求情報入力手段と、前記入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定する文書公開判定手段と、前記文書公開判定手段の判定結果に応じて前記閲覧対象の文書を公開する文書公開手段とを備えることを特徴とする文書管理装置。

【請求項2】 前記セキュリティ情報は、前記セキュリティの優先順位を示す階層と、文書閲覧を許可する許可メンバをグループ化するためのセキュリティ集合と、前記許可メンバと、前記文書の公開境界条件とを含む情報からなることを特徴とする請求項1記載の文書管理装置。

【請求項3】 前記セキュリティ情報に含まれる前記階層、前記セキュリティ集合、前記許可メンバ、前記文書の公開境界条件の各情報は個別に選択可能であることを特徴とする請求項2記載の文書管理装置。

【請求項4】 前記セキュリティ情報選択手段は、前記選択した公開許可条件に応じて前記セキュリティ情報の選択範囲を設定し、該設定された選択範囲の中から前記セキュリティ情報を選択することを特徴とする請求項3記載の文書管理装置。

【請求項5】 前記閲覧要求情報は、前記閲覧希望メンバが所属するセキュリティ集合およびそのセキュリティ階層を含むことを特徴とする請求項2ないし4のいずれか1つに記載の文書管理装置。

【請求項6】 前記文書公開判定手段は、前記文書に付加された公開許可条件に従い入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定することを特徴とする請求項1または5記載の文書管理装置。

【請求項7】 文書格納手段に格納された文書を公開可能に管理する文書管理方法において、前記文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録する工程と、前記登録されたセキュリティ情報の中から前記文書に付加するセキュリティ情報を選択する工程と、前記選択したセキュリティ情報を前記文書に対応付けて付加する工程と、前記文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力す

る工程と、前記入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定する工程と、前記判定結果に応じて前記閲覧対象の文書を公開する工程とを有することを特徴とする文書管理方法。

【請求項8】 前記セキュリティ情報は、前記セキュリティの優先順位を示す階層と、文書閲覧を許可する許可メンバをグループ化するためのセキュリティ集合と、前記許可メンバと、前記文書の公開境界条件とを含む情報からなることを特徴とする請求項7記載の文書管理方法。

【請求項9】 前記セキュリティ情報に含まれる前記階層、前記セキュリティ集合、前記許可メンバ、前記文書の公開境界条件の各情報は個別に選択可能であることを特徴とする請求項8記載の文書管理方法。

【請求項10】 前記選択した公開許可条件に応じて前記セキュリティ情報の選択範囲を設定し、該設定された選択範囲の中から前記セキュリティ情報を選択することを特徴とする請求項9記載の文書管理方法。

【請求項11】 前記閲覧要求情報は、前記閲覧希望メンバが所属するセキュリティ集合およびそのセキュリティ階層を含むことを特徴とする請求項8ないし10のいずれか1つに記載の文書管理方法。

【請求項12】 前記文書に付加された公開許可条件に従い入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定することを特徴とする請求項7または11記載の文書管理方法。

【請求項13】 文書格納手段に格納された文書を公開可能に管理する文書管理システムを情報処理装置上に構築するためのプログラムを格納した記憶媒体において、前記プログラムは、前記文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録するセキュリティ情報登録モジュールと、前記登録されたセキュリティ情報の中から前記文書に付加するセキュリティ情報を選択するセキュリティ情報選択モジュールと、前記選択したセキュリティ情報を前記文書に対応付けて付加するセキュリティ情報付加モジュールと、前記文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する閲覧要求情報入力モジュールと、前記入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定する文書公開判定モジュールと、前記文書公開判定モジュールの判定結果に応じて前記閲覧対象の文書を公開する文書公開モジュールとを有することを特徴とする記憶媒体。

【請求項14】 前記セキュリティ情報は、前記セキュリティの優先順位を示す階層と、文書閲覧を許可する許可メンバをグループ化するためのセキュリティ集合と、

前記許可メンバと、前記文書の公開境界条件とを含む情報からなることを特徴とする請求項1記載の記憶媒体。

【請求項15】 前記セキュリティ情報に含まれる前記階層、前記セキュリティ集合、前記許可メンバ、前記文書の公開境界条件の各情報は個別に選択可能であることを特徴とする請求項14記載の記憶媒体。

【請求項16】 前記セキュリティ情報選択モジュールは、前記選択した公開許可条件に応じて前記セキュリティ情報の選択範囲を設定し、該設定された選択範囲の中 10 から前記セキュリティ情報を選択することを特徴とする請求項15記載の記憶媒体。

【請求項17】 前記閲覧要求情報は、前記閲覧希望メンバが所属するセキュリティ集合およびそのセキュリティ階層を含むことを特徴とする請求項14ないし16のいずれか1つに記載の記憶媒体。

【請求項18】 前記文書公開判定モジュールは、前記文書に付加された公開許可条件に従い入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して 20 公開可能な否かを判定することを特徴とする請求項13または17記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、文書格納手段に格納された文書を公開可能に管理する文書管理装置、文書管理方法および記憶媒体に関する。

【0002】

【従来の技術】従来、スキャナなどにより読み込んで得られたイメージデータ、ワードプロセッサにより作成された文書データなどの文書ファイルを管理する文書管理方法として、前記文書ファイルをセキュリティ情報と関連付けて記憶し、入力された情報とセキュリティ情報とを照合することによって前記文書ファイルの公開を行うものがある。ここで、セキュリティ情報は文書ファイルの公開の度合を表す情報であり、このセキュリティ情報は、対応する文書ファイルに対してその公開の度合に応じて付加される。

【0003】

【発明が解決しようとする課題】しかしながら、上述した従来の文書管理方法では、文書ファイルに対するセキュリティを堅固にするほど、文書ファイルに対するセキュリティの区分が細分化され、文書ファイルに付加するセキュリティ情報としてどの段階のセキュリティ情報を付加すればよいのかを判断し難くなる。その結果、文書ファイルに対して適正なセキュリティ情報を付加することができず、文書ファイルに対して適正なセキュリティ管理を行うことが困難になる。

【0004】本発明の目的は、文書に対するセキュリティの設定および管理を容易に行うことができる文書管理 50

装置、文書管理方法および記憶媒体を提供することにある。

【0005】

【課題を解決するための手段】請求項1記載の発明は、文書格納手段に格納された文書を公開可能に管理する文書管理装置において、前記文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録するセキュリティ情報登録手段と、前記登録されたセキュリティ情報の中から前記文書に付加するセキュリティ情報を選択するセキュリティ情報選択手段と、前記選択したセキュリティ情報を前記文書に対応付けて付加するセキュリティ情報付加手段と、前記文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する閲覧要求情報入力手段と、前記入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定する文書公開判定手段と、前記文書公開判定手段の判定結果に応じて前記閲覧対象の文書を公開する文書公開手段とを備えることを特徴とする。

【0006】請求項2記載の発明は、請求項1記載の文書管理装置において、前記セキュリティ情報は、前記セキュリティの優先順位を示す階層と、文書閲覧を許可する許可メンバをグループ化するためのセキュリティ集合と、前記許可メンバと、前記文書の公開境界条件とを含む情報からなることを特徴とする。

【0007】請求項3記載の発明は、請求項2記載の文書管理装置において、前記セキュリティ情報に含まれる前記階層、前記セキュリティ集合、前記許可メンバ、前記文書の公開境界条件の各情報は個別に選択可能であることを特徴とする。

【0008】請求項4記載の発明は、請求項3記載の文書管理装置において、前記セキュリティ情報選択手段は、前記選択した公開許可条件に応じて前記セキュリティ情報の選択範囲を設定し、該設定された選択範囲の中から前記セキュリティ情報を選択することを特徴とする。

【0009】請求項5記載の発明は、請求項2ないし4のいずれか1つに記載の文書管理装置において、前記閲覧要求情報は、前記閲覧希望メンバが所属するセキュリティ集合およびそのセキュリティ階層を含むことを特徴とする。

【0010】請求項6記載の発明は、請求項1または5記載の文書管理装置において、前記文書公開判定手段は、前記文書に付加された公開許可条件に従い入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定することを特徴とする。

【0011】請求項7記載の発明は、文書格納手段に格納された文書を公開可能に管理する文書管理方法において、前記文書に対するセキュリティの度合を決定するた

めのセキュリティ情報を登録する工程と、前記登録されたセキュリティ情報の中から前記文書に付加するセキュリティ情報を選択する工程と、前記選択したセキュリティ情報を前記文書に対応付けて付加する工程と、前記文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する工程と、前記入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定する工程と、前記判定結果に応じて前記閲覧対象の文書を公開する工程とを有することを特徴とする。

【0012】請求項8記載の発明は、請求項7記載の文書管理方法において、前記セキュリティ情報は、前記セキュリティの優先順位を示す階層と、文書閲覧を許可する許可メンバをグループ化するためのセキュリティ集合と、前記許可メンバと、前記文書の公開境界条件とを含む情報からなることを特徴とする。

【0013】請求項9記載の発明は、請求項8記載の文書管理方法において、前記セキュリティ情報に含まれる前記階層、前記セキュリティ集合、前記許可メンバ、前記文書の公開境界条件の各情報は個別に選択可能であることを特徴とする。

【0014】請求項10記載の発明は、請求項9記載の文書管理方法において、前記選択した公開許可条件に応じて前記セキュリティ情報の選択範囲を設定し、該設定された選択範囲の中から前記セキュリティ情報を選択することを特徴とする。

【0015】請求項11記載の発明は、請求項8ないし10のいずれか1つに記載の文書管理方法において、前記閲覧要求情報は、前記閲覧希望メンバが所属するセキュリティ集合およびそのセキュリティ階層を含むことを特徴とする。

【0016】請求項12記載の発明は、請求項7または11記載の文書管理方法において、前記文書に付加された公開許可条件に従い入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定することを特徴とする。

【0017】請求項13記載の発明は、文書格納手段に格納された文書を公開可能に管理する文書管理システムを情報処理装置上に構築するためのプログラムを格納した記憶媒体において、前記プログラムは、前記文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録するセキュリティ情報登録モジュールと、前記登録されたセキュリティ情報の中から前記文書に付加するセキュリティ情報を選択するセキュリティ情報選択モジュールと、前記選択したセキュリティ情報を前記文書に対応付けて付加するセキュリティ情報付加モジュールと、前記文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する閲覧要求情報入力

モジュールと、前記入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定する文書公開判定モジュールと、前記文書公開判定モジュールの判定結果に応じて前記閲覧対象の文書を公開する文書公開モジュールとを有することを特徴とする。

【0018】請求項14記載の発明は、請求項13記載の記憶媒体において、前記セキュリティ情報は、前記セキュリティの優先順位を示す階層と、文書閲覧を許可する許可メンバをグループ化するためのセキュリティ集合と、前記許可メンバと、前記文書の公開境界条件とを含む情報からなることを特徴とする。

【0019】請求項15記載の発明は、請求項14記載の記憶媒体において、前記セキュリティ情報に含まれる前記階層、前記セキュリティ集合、前記許可メンバ、前記文書の公開境界条件の各情報は個別に選択可能であることを特徴とする。

【0020】請求項16記載の発明は、請求項15記載の記憶媒体において、前記セキュリティ情報選択モジュールは、前記選択した公開許可条件に応じて前記セキュリティ情報の選択範囲を設定し、該設定された選択範囲の中から前記セキュリティ情報を選択することを特徴とする。

【0021】請求項17記載の発明は、請求項14ないし16のいずれか1つに記載の記憶媒体において、前記閲覧要求情報は、前記閲覧希望メンバが所属するセキュリティ集合およびそのセキュリティ階層を含むことを特徴とする。

【0022】請求項18記載の発明は、請求項13または17記載の記憶媒体において、前記文書公開判定モジュールは、前記文書に付加された公開許可条件に従い入力された閲覧要求情報と前記文書に付加されたセキュリティ情報とを照合して前記閲覧対象文書を前記閲覧希望メンバに対して公開可能な否かを判定することを特徴とする。

【0023】

【発明の実施の形態】以下に、本発明の実施の形態について図を参照しながら説明する。

【0024】図1は本発明の文書管理装置の実施の一形態の構成を示すブロック図である。

【0025】文書管理装置は、図1に示すように、セキュリティ階層登録手段101、セキュリティ集合登録手段102、セキュリティメンバ登録手段103および文書登録手段105を備える。セキュリティ階層登録手段101は、ユーザにより指定されるセキュリティの優先順位を示すセキュリティ階層をセキュリティ情報記憶手段104に登録する処理を行う。セキュリティ集合登録手段102は、ユーザにより指定される、セキュリティメンバをグループ化するためのセキュリティ集合をセキ

セキュリティ情報記憶手段104に登録する処理を行う。セキュリティメンバ登録手段103は、ユーザにより指定される本文書管理装置を利用するメンバをセキュリティ情報記憶手段104に登録する処理を行う。ここで、メンバはセキュリティ階層およびセキュリティ集合と対応付けてセキュリティ情報記憶手段104に記憶される。

【0026】文書登録手段105は、ユーザにより指定された文書データを文書記憶手段106に登録するとともに、文書セキュリティ公開方法選択手段107に対して文書の公開方法を選択することを要求する。文書セキュリティ公開方法選択手段107は、文書登録手段105からの要求に従い登録する文書データの公開方法をユーザに選択させるための処理を行う。ここでは、公開方法の選択肢としては、「登録者のみ」、「指定の階層以上」、「指定の集合のみ」、「指定の階層以上かつ指定の集合のみ」、「指定階層以上または指定の集合のみ」が設定されている。

【0027】そして、文書セキュリティ集合選択手段108により、セキュリティ情報記憶手段104の中から文書データに付加するセキュリティ集合を選択するための処理を行う。この処理では、セキュリティ情報記憶手段104に登録されているセキュリティ集合を読み出してユーザ操作により選択可能に表示装置(図示せず)に表示し、この表示されたセキュリティ集合の中からユーザ操作に選択されたセキュリティ集合を登録する文書データに対応付けて文書セキュリティ情報記憶手段110に格納する。ここで、選択可能なセキュリティ集合としてはユーザが所属するセキュリティ集合である。

【0028】また、文書セキュリティ階層選択手段109により、セキュリティ情報記憶手段104の中から登録する文書データに対して付加するセキュリティ階層を選択するための処理を行う。この処理では、セキュリティ情報記憶手段104に登録されているセキュリティ階層を読み出してユーザ操作により選択可能に表示装置(図示せず)に表示し、この表示されたセキュリティ階層の中からユーザ操作に選択されたセキュリティ階層を登録する文書データに対応付けて文書セキュリティ情報記憶手段110に格納する。ここで、選択可能なセキュリティ階層としては、ユーザが所属するセキュリティ階層より下位のセキュリティ階層である。

【0029】文書記憶手段106に登録された文書データを読み出して参照する際には、参照文書選択手段111により閲覧を希望するユーザから該ユーザ名および文書名を少なくとも含む閲覧要求情報を入力する。この閲覧要求情報はセキュリティ判定手段112に与えられ、セキュリティ判定手段112は、閲覧要求情報とセキュリティ情報記憶手段104および文書セキュリティ情報記憶手段110の各情報とを照合することによって閲覧を希望する文書をユーザに対して公開可能か否かを判定する。この判定結果は参照文書表示手段113に与えら

れ、参照文書表示手段113は、上記判定結果が公開可能であることを示すときには、対応する文書データを文書記憶手段106から読み出して表示装置に表示する。

【0030】次に、本文書管理装置のハードウェア構成について図2を参照しながら説明する。図2は図1の文書管理装置のハードウェア構成を示すブロック図である。

【0031】文書管理装置のハードウェア構成においては、図2に示すように、ROM(リードオンリーメモリ)207に格納されているプログラムに従って対応する処理を実行するCPU201と、CPU201の演算処理の結果を一時的に保持するなどの作業領域を提供するRAM(ランダムアクセスメモリ)208とを備える。CPU201には、ROM207およびRAM208とともに、キーボード202(KB)、マウス203、表示装置204、フロッピディスク装置(FDD)205、スキャナ206、ハードディスク装置(HDD)209がバス210を介して接続されている。

【0032】キーボード202は登録するセキュリティ情報などを入力するために使用され、マウス203は、表示装置204上に表示されるセキュリティ階層、セキュリティ集合の選択操作などに使用される。表示装置204は、セキュリティ階層、セキュリティ集合の選択画面、CPU201の演算処理の結果などを表示するCRT、液晶表示装置などからなる。フロッピディスク装置205は、登録する文書、検索した文書などをフロッピディスクに書き込み、またフロッピディスクから文書データなどを読み出すなどの書き込み、読み出し動作を行う。スキャナ206は、原稿などから画像を読み取り、この読み取った画像は文書データとしてハードディスク装置209に登録される。ハードディスク装置209は、用語情報、文書データなどを格納する。

【0033】ここで、上記ROM207に格納されているプログラムには、文書管理プログラムが含まれ、この文書管理プログラムは、上述したセキュリティ階層登録手段101、セキュリティ集合登録手段102、セキュリティメンバ登録手段103、文書登録手段105、文書セキュリティ公開方法選択手段107、文書セキュリティ集合選択手段108、文書セキュリティ階層選択手段109、参照文書選択手段111、セキュリティ判定手段112および参照文書表示手段113を構成する。また、ハードディスク装置209は、セキュリティ情報記憶手段104、文書記憶手段106、文書セキュリティ情報記憶手段110を構成する。

【0034】次に、本文書管理装置のハードディスク装置209における文書データ、セキュリティ情報などの管理について図3を参照しながら説明する。図3は図2の文書管理装置のハードディスク装置209における文書データ、セキュリティ情報などの管理方法を示す図である。

【0035】ハードディスク装置209における文書データ、セキュリティ情報などの管理においては、ハードディスク装置209にセキュリティ情報領域、文書データ領域を割り当て、それぞれの領域を管理領域301の情報をを用いて管理する。この管理領域301にはセキュリティ情報格納先が設けられ、このセキュリティ情報格納先には、セキュリティメンバの情報を格納する領域302が含まれる。この領域302には、セキュリティメンバのメンバ名、セキュリティメンバ本人確認用パスワード、セキュリティメンバ所属のセキュリティ階層を格納した領域のアドレスを示す階層格納先、セキュリティメンバ所属のセキュリティ集合を格納した領域のアドレスを示す集合格納先が含まれる。領域302の階層格納先のアドレスに対応する領域305には階層順位、階層名が格納されている。領域302の集合格納先のアドレスに対応する領域303には、セキュリティ集合を格納した領域を示すアドレスを格納する。

【0036】また、管理領域301には文書情報格納先が設けられ、この文書情報格納先には、登録者格納先、文書格納先、文書名、セキュリティ階層を格納した領域のアドレスを示す階層格納先、背きゅうり定収号を格納した領域のアドレスを示す集合格納先、文書公開方法を格納する領域306が含まれる。ここで、文書格納先は登録した文書データを格納した領域307のアドレスを示す。

【0037】本例では、文書「Next Year Budget」に対して登録者「Andrew」、階層「External」、集合「集合なし」、公開方法「指定の階層以上」が付加されている。よって、文書「Next Year Budget」は階層「External」以上の階層のメンバに対して公開される。また、文書「Products Invoice」に対しては、登録者「Mark」、階層「Corporate」、集合「Development」、公開方法「指定の階層以上または指定の集合のみ」が付加されている。よって、文書「Products Invoice」は階層「Corporate」以上の階層のメンバまたは集合「Development」に所属するメンバに対して公開される。

【0038】次に、セキュリティ階層、セキュリティ集合、セキュリティメンバの各情報の登録画面について図4ないし図6を参照しながら説明する。図4は図1の文書管理装置におけるセキュリティ階層登録画面の一例を示す図、図5は図1の文書管理装置におけるセキュリティ集合登録画面の一例を示す図、図6は図1の文書管理装置におけるセキュリティメンバ登録画面の一例を示す図である。

【0039】セキュリティ階層を登録する際には、例えば図4に示す登録画面が用いられる。本例では、既に登録されているセキュリティ階層の一覧401が表示され、この画面上で新たなセキュリティ階層を入力することによって新たなセキュリティ階層を登録することが可能である。なお、ここでは、この新たなセキュリティ階

層の登録操作についての説明は省略する。

【0040】セキュリティ集合を登録する際には、例えば図5に示す登録画面が用いられる。本例では、既に登録されているセキュリティ集合の一覧501とともに、セキュリティ集合に所属するメンバの一覧502が表示され、この画面上で新たなセキュリティ集合を入力することによって新たなセキュリティ集合を登録することが可能である。なお、ここでは、この新たなセキュリティ集合の登録操作についての説明は省略する。

【0041】セキュリティメンバを登録する際には、例えば図6に示す登録画面が用いられる。本例では、既に登録されているセキュリティメンバの一覧601とともに、セキュリティメンバが所属するセキュリティ集合の一覧602が表示され、この画面上で新たなセキュリティメンバを入力することによって新たなセキュリティ集合を登録することが可能である。なお、ここでは、この新たなセキュリティメンバの登録操作についての説明は省略する。

【0042】次に、登録する文書データに対して付加するセキュリティ情報を選択するための画面について図7を参照しながら説明する。図7は図1の文書管理装置における登録文書データに対して付加するセキュリティ情報を選択するための画面例を示す図である。

【0043】登録する文書データにセキュリティ情報を付加する際には、例えば図7に示す画面が用いられる。この画面においては、予め登録されている公開方法の選択欄701、登録する文書に対するセキュリティ集合の入力欄702およびセキュリティ階層の入力欄703が表示される。この画面上で選択された公開方法、セキュリティ集合、セキュリティ階層は登録する文書データに対応付けて文書セキュリティ情報記憶手段110に登録される。

【0044】次に、本文書管理装置における全体動作について図8を参照しながら説明する。図8は図1の文書管理装置における全体動作を示すフローチャートである。

【0045】本文処理管理装置では、図8に示すように、まずステップS801においてキーボード202またはマウス203からの操作の受付を行う。そして、ステップS802に進み、この受け付けた操作の指示内容を判定する。この受け付けた操作の指示内容がセキュリティ情報登録であるときには、ステップS803に進み、セキュリティ情報登録処理を行う。このセキュリティ情報登録処理の詳細については後述する。セキュリティ情報登録処理が終了すると、再度上記ステップS801に戻る。

【0046】受け付けた操作の指示内容が文書登録であるときには、ステップS804に進み、文書登録処理を行う。この文書登録処理の詳細については後述する。文書登録処理が終了すると、再度上記ステップS801に

戻る。受け付けた操作の指示内容が文書参照であるときには、ステップS805に進み、文書参照処理を行う。この文書参照処理の詳細については後述する。文書参照処理が終了すると、再度上記ステップS801に戻る。

【0047】次に、セキュリティ情報登録処理、文書登録処理、文書参照処理について図9ないし図11を参照しながら説明する。図9は図8のステップS803におけるセキュリティ情報登録処理の手順を示すフローチャート、図10は図8のステップS804における文書登録処理の手順を示すフローチャート、図11は図8のステップS805における文書参照処理の手順を示すフローチャートである。

【0048】セキュリティ情報登録処理では、図9に示すように、まずステップS901においてキーボード202またはマウス203からの操作の受付を行う。そして、ステップS902に進み、受け付けた操作の指示内容を判定する。受け付けた操作の指示内容がセキュリティ階層受付であるときには、ステップS903に進み、セキュリティ階層の受付を行う。このセキュリティ階層の受付においては、図4に示す登録画面を表示し、この登録画面上でキーボード202またはマウス203の操作により入力されたセキュリティ階層名とその順位を受け付ける。続くステップS904では、受け付けたセキュリティ階層名とその順位をハードディスク装置209（図1のセキュリティ情報記憶手段104）に登録するセキュリティ階層登録処理を行う。そして、上記ステップS901に戻るかまたは本処理を終了する。ここで、上記ステップS901に戻るか本処理を終了するかは、セキュリティ階層登録処理の実行後に表示装置204に選択画面を表示し、この選択画面においてそれらのいずれかを選択するように構成することが可能である。

【0049】受け付けた操作の指示内容がセキュリティ集合受付であるときには、ステップS905に進み、セキュリティ集合受付を行う。このセキュリティ集合受付においては、図5に示す登録画面を表示し、この登録画面上でキーボード202またはマウス203の操作により入力されたセキュリティ集合名を受け付ける。続くステップS906では、受け付けたセキュリティ集合名をハードディスク装置209（図1のセキュリティ情報記憶手段104）に登録するセキュリティ集合登録処理を行う。そして、上記ステップS901に戻るかまたは本処理を終了する。

【0050】受け付けた操作の指示内容がセキュリティメンバ受付であるときには、ステップS907に進み、セキュリティメンバ受付を行う。このセキュリティメンバ受付においては、図7に示す登録画面を表示し、この登録画面上でキーボード202またはマウス203の操作により入力されたセキュリティメンバ名を受け付ける。続くステップS908では、受け付けたセキュリティメンバをハードディスク装置209（図1のセキュリ

ティ情報記憶手段104）に登録するセキュリティメンバ登録処理を行う。そして、上記ステップS901に戻るかまたは本処理を終了する。

【0051】次に、文書登録処理について説明する。本処理では、図10に示すように、まずステップS1001においてセキュリティメンバすなわちユーザのログインを受け付け、続くステップS1002でユーザにより指定された文書データを読み込み、そしてステップS1003で読み込んだ文書データに対する公開方法を選択するための画面（図7に示す画面）を表示し、該画面上で選択された公開方法を入力する。ここで、登録する文書データに対する公開方法の選択肢としては、上述したように、「登録者のみ」、「指定の階層以上」、「指定の集合のみ」、「指定の階層以上かつ指定の集合のみ」、「指定階層以上または指定の集合のみ」が設定されている。

【0052】次いで、ステップS1004に進み、選択された公開方法を判定する。ここで、選択された公開方法が「登録者のみ」であるときには、ステップS1009に進み、この登録する文書データに対する公開方法として「登録者のみ」をハードディスク装置209の所定領域（図1に示す文書セキュリティ情報記憶手段110）に登録し、続くステップS1010で指定した文書データをハードディスク装置209の所定領域（図1に示す文書記憶手段106）に格納する。そして本処理を終了する。

【0053】選択された公開方法が「指定の階層以上」であるときには、ステップS1005に進み、ログインしたセキュリティメンバが所属するセキュリティ階層より下位の階層の中から選択されたセキュリティ階層を受け付ける。次いで、ステップS1009に進み、登録する文書データに対する公開方法である「指定の階層以上」および受け付けたセキュリティ階層をハードディスク装置209の所定領域（図1に示す文書セキュリティ情報記憶手段110）に登録し、続くステップS1010で指定した文書データをハードディスク装置209の所定領域（図1に示す文書記憶手段106）に格納する。そして本処理を終了する。

【0054】選択された公開方法が「指定の集合のみ」であるときには、ステップS1006に進み、ログインしたセキュリティメンバが所属するセキュリティ集合の中から選択されたセキュリティ集合を受け付ける。次いで、ステップS1009に進み、登録する文書データに対する公開方法である「指定の集合のみ」および受け付けたセキュリティ集合のみをハードディスク装置209の所定領域（図1に示す文書セキュリティ情報記憶手段110）に登録し、続くステップS1010で指定した文書データをハードディスク装置209の所定領域（図1に示す文書記憶手段106）に格納する。そして本処理を終了する。



【0055】選択された公開方法が「指定の階層以上かつ指定の集合のみ」または「指定階層以上または指定の集合のみ」であるときには、ステップS1007に進み、ログインしたセキュリティメンバが所属するセキュリティ階層より下位の階層の中から選択されたセキュリティ階層を受け付け、続くステップS1008で、ログインしたセキュリティメンバが所属するセキュリティ集合の中から選択されたセキュリティ集合を受け付ける。次いで、ステップS1009に進み、登録する文書データに対する公開方法である「指定の階層以上かつ指定の集合のみ」または「指定階層以上または指定の集合のみ」と、受け付けたセキュリティ階層およびセキュリティ集合をハードディスク装置209の所定領域（図1に示す文書セキュリティ情報記憶手段110）に登録し、続くステップS1010で指定した文書データをハードディスク装置209の所定領域（図1に示す文書記憶手段106）に格納する。そして本処理を終了する。

【0056】次に、文書参照処理について説明する。本処理では、図11に示すように、まずステップS1101で、セキュリティメンバのログインを受け付け、続くステップS1102において閲覧希望対象の文書名を入力し、そしてステップS1103で入力した文書名の文書データの参照が可能か否かを判定する。ここで、閲覧希望対象の文書データの公開方法として「登録者のみ」が設定されているときには、ログインしたセキュリティメンバと閲覧希望対象の文書データに付加されているセキュリティメンバとが同一であるか否かを判定し、ログインしたセキュリティメンバと閲覧希望対象の文書データに付加されているセキュリティメンバとが同一であるときには、ステップS1104に進み、この文書データをハードディスク装置209（図1の文書記憶手段106）から読み出して表示装置204に表示し、そして本処理を終了する。これに対し、ログインしたセキュリティメンバと閲覧希望対象の文書データに付加されているセキュリティメンバとが同一でないときには、この文書データがログインしたセキュリティメンバに対して非公開の文書データであると判断して本処理を終了する。

【0057】また、閲覧希望対象の文書データの公開方法として「指定の階層以上」が設定されているときには、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上であるか否かを判定し、ログインしたセキュリティメンバのセキュリティ階層が文書データに付加されているセキュリティ階層以上であるときには、ステップS1104に進み、この文書データをハードディスク装置209（図1の文書記憶手段106）から読み出して表示装置204に表示する。これに対し、ログインしたセキュリティメンバのセキュリティ階層が文書データに付加されているセキュリティ階層以上でないときには、この文書データがログインしたセキュリティメン

バに対して非公開の文書データであると判断して本処理を終了する。

【0058】さらに、閲覧希望対象の文書データの公開方法として「指定の集合のみ」が設定されているときには、ログインしたセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属しているか否かを判定し、ログインしたセキュリティメンバが文書データに付加されているセキュリティ集合に所属しているときには、ステップS1104に進み、この文書データをハードディスク装置209（図1の文書記憶手段106）から読み出して表示装置204に表示する。これに対し、ログインしたセキュリティメンバが文書データに付加されているセキュリティ集合に所属していないときには、この文書データがログインしたセキュリティメンバに対して非公開の文書データであると判断して本処理を終了する。

【0059】さらに、閲覧希望対象の文書データの公開方法として「指定の階層以上かつ指定の集合のみ」が設定されているときには、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上でありかつこのセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属しているか否かを判定し、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上でありかつこのセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属しているときには、ステップS1104に進み、この文書データをハードディスク装置209（図1の文書記憶手段106）から読み出して表示装置204に表示する。これに対し、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上でありかつこのセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属していないときには、この文書データがログインしたセキュリティメンバに対して非公開の文書データであると判断して本処理を終了する。

【0060】さらに、閲覧希望対象の文書データの公開方法として「指定の階層以上または指定の集合のみ」が設定されているときには、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上またはこのセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属しているか否かを判定し、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上またはこのセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属しているときには、ステップS1104に進み、この

文書データをハードディスク装置209（図1の文書記憶手段106）から読み出して表示装置204に表示する。これに対し、ログインしたセキュリティメンバのセキュリティ階層が閲覧希望対象の文書データに付加されているセキュリティ階層以上またはこのセキュリティメンバが閲覧希望対象の文書データに付加されているセキュリティ集合に所属していないときには、この文書データがログインしたセキュリティメンバに対して非公開の文書データであると判断して本処理を終了する。

【0061】このように本実施の形態では、文書データに付加するセキュリティ情報を予め登録し、登録されたセキュリティ情報の中から文書データに付加するセキュリティ情報を選択して記憶し、セキュリティメンバおよび文書名を入力し、この入力された情報と文書データに対応付けて記憶されているセキュリティ情報とを照合することによってこの文書データが公開可能か否かを判定し、この判定結果に応じて文書データの公開を行うから、文書データに対するセキュリティの設定および管理を容易に行うことができる。

【0062】また、文書に対するセキュリティ情報を階層的に分類して登録することによって、文書データに対するセキュリティをより高めることができる。

【0063】なお、本実施の形態では、各ブロックを同一の装置上で構成した例を示したが、ネットワーク上に分散したコンピュータや処理装置を用いて各部を構成することも可能である。

【0064】さらに、本実施の形態では、各ブロックを構成するためのプログラムをROMに格納しているが、これに代えて他の記憶媒体に格納してもよい。例えば、ハードディスク装置などに上記プログラムを格納し、このプログラムを読み出して実行するように構成することもできる。また、CDROM、MO、FD、メモリカードなどの記憶媒体から上記プログラムを供給するように構成してよい。また、各ブロックに対応する処理を実行するハードウェア回路で構成するようにしてもよい。

【0065】

【発明の効果】以上説明したように、本発明の文書管理装置によれば、文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録するセキュリティ情報登録手段と、登録されたセキュリティ情報の中から文書に付加するセキュリティ情報を選択するセキュリティ情報選択手段と、選択したセキュリティ情報を文書に対応付けて付加するセキュリティ情報付加手段と、文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する閲覧要求情報入力手段と、入力された閲覧要求情報と文書に付加されたセキュリティ情報とを照合して閲覧対象文書を閲覧希望メンバに対して公開可能な否かを判定する文書公開判定手段と、文書公開判定手段の判定結果に応じて前記閲覧対象の文書を公開する文書公開手段とを備えるから、文書に対するセキュリ

ティの設定および管理を容易に行うことができる。

【0066】本発明の文書管理方法によれば、文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録する工程と、登録されたセキュリティ情報の中から文書に付加するセキュリティ情報を選択する工程と、選択したセキュリティ情報を前記文書に対応付けて付加する工程と、文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する工程と、入力された閲覧要求情報と文書に付加されたセキュリティ情報とを照合して閲覧対象文書を閲覧希望メンバに対して公開可能な否かを判定する工程と、判定結果に応じて閲覧対象の文書を公開する工程とを有するから、文書に対するセキュリティの設定および管理を容易に行うことができる。

【0067】本発明の記憶媒体によれば、プログラムは、文書に対するセキュリティの度合を決定するためのセキュリティ情報を登録するセキュリティ情報登録モジュールと、登録されたセキュリティ情報の中から文書に付加するセキュリティ情報を選択するセキュリティ情報選択モジュールと、選択したセキュリティ情報を文書に対応付けて付加するセキュリティ情報付加モジュールと、文書閲覧希望メンバおよび閲覧対象文書を少なくとも含む閲覧要求情報を入力する閲覧要求情報入力モジュールと、入力された閲覧要求情報と文書に付加されたセキュリティ情報とを照合して閲覧対象文書を閲覧希望メンバに対して公開可能な否かを判定する文書公開判定モジュールと、文書公開判定モジュールの判定結果に応じて閲覧対象の文書を公開する文書公開モジュールとを有するから、文書に対するセキュリティの設定および管理を容易に行うことができる。

【図面の簡単な説明】

【図1】本発明の文書管理装置の実施の一形態の構成を示すブロック図である。

【図2】図1の文書管理装置のハードウェア構成を示すブロック図である。

【図3】図2の文書管理装置のハードディスク装置209における文書データ、セキュリティ情報などの管理方法を示す図である。

【図4】図1の文書管理装置におけるセキュリティ階層登録画面の一例を示す図である。

【図5】図1の文書管理装置におけるセキュリティ集合登録画面の一例を示す図である。

【図6】図1の文書管理装置におけるセキュリティメンバ登録画面の一例を示す図である。

【図7】図1の文書管理装置における登録文書データに対して付加するセキュリティ情報を選択するための画面例を示す図である。

【図8】図1の文書管理装置における全体動作を示すフローチャートである。

【図9】図8のステップS803におけるセキュリティ

17

情報登録処理の手順を示すフローチャートである。

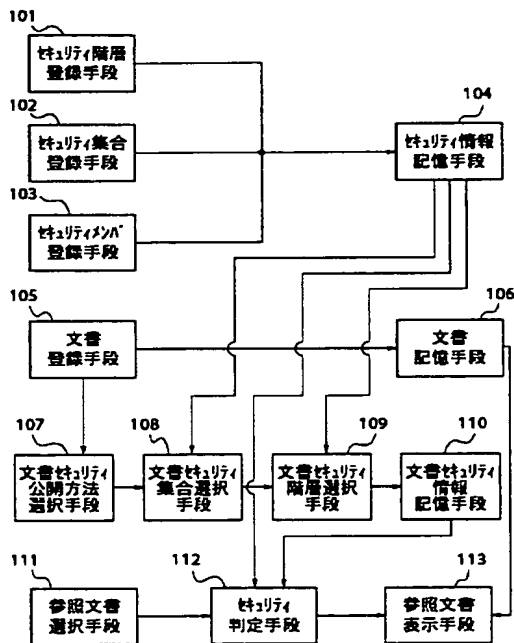
【図10】図8のステップS804における文書登録処理の手順を示すフローチャートである。

【図11】図8のステップS805における文書参照処理の手順を示すフローチャートである。

【符号の説明】

- 101 セキュリティ階層登録手段
- 102 セキュリティ集合登録手段
- 103 セキュリティメンバー登録手段
- 104 セキュリティ情報記憶手段
- 105 文書登録手段
- 106 文書記憶手段
- 107 文書セキュリティ公開方法選択手段
- 108 文書セキュリティ集合選択手段
- 109 文書セキュリティ階層選択手段
- 110 文書セキュリティ情報記憶手段
- 111 参照文書選択手段
- 112 セキュリティ判定手段
- 113 参照文書表示手段

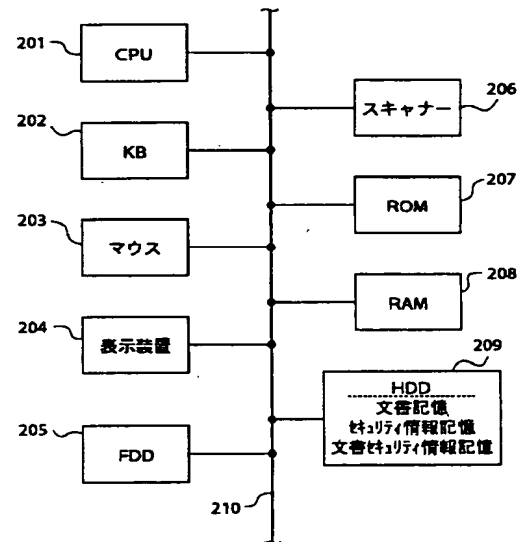
【図1】



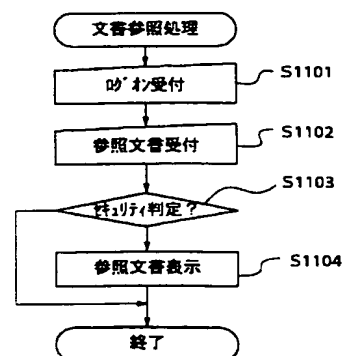
18

- 108 文書セキュリティ集合選択手段
- 109 文書セキュリティ階層選択手段
- 110 文書セキュリティ情報記憶手段
- 111 参照文書選択手段
- 112 セキュリティ判定手段
- 113 参照文書表示手段
- 201 CPU
- 202 キーボード
- 203 マウス
- 204 表示装置
- 207 ROM
- 208 RAM
- 209 ハードディスク装置

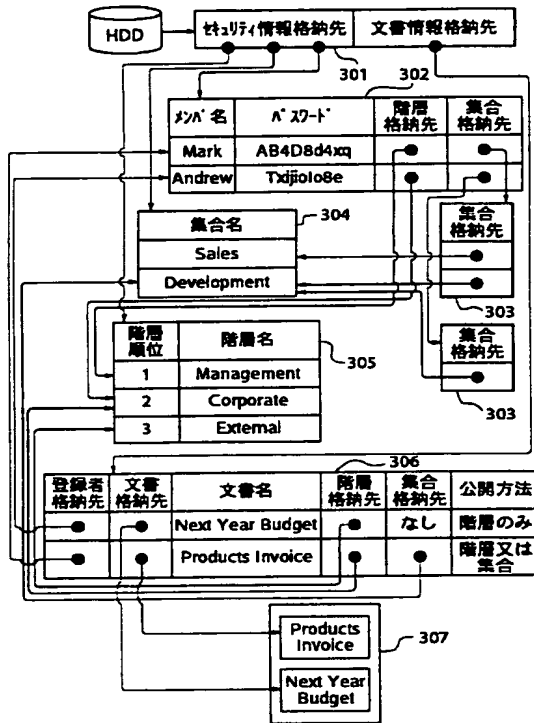
【図2】



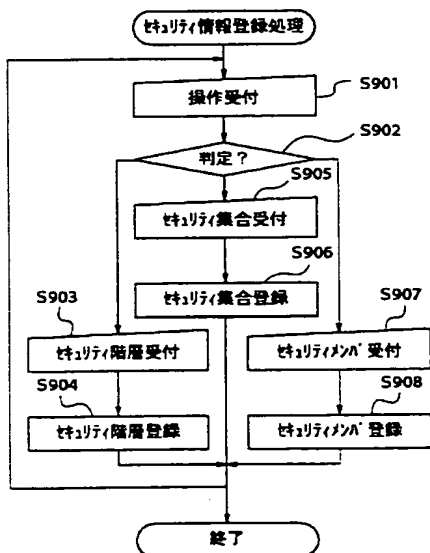
【図11】



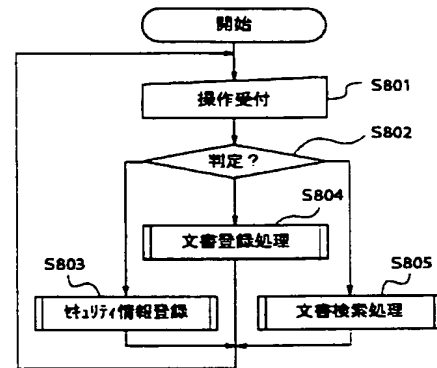
【図3】



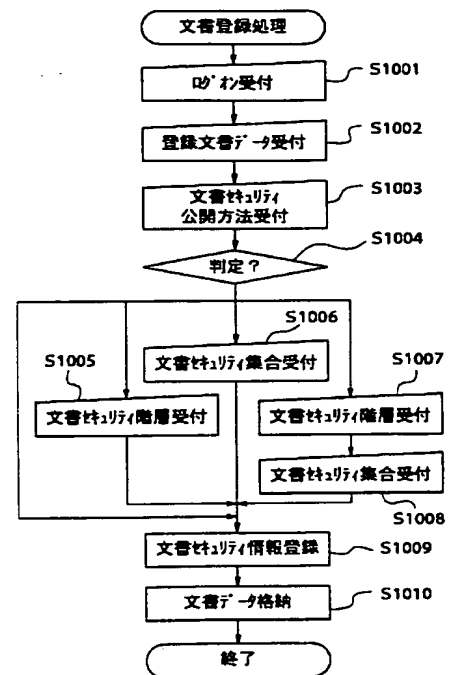
【図9】



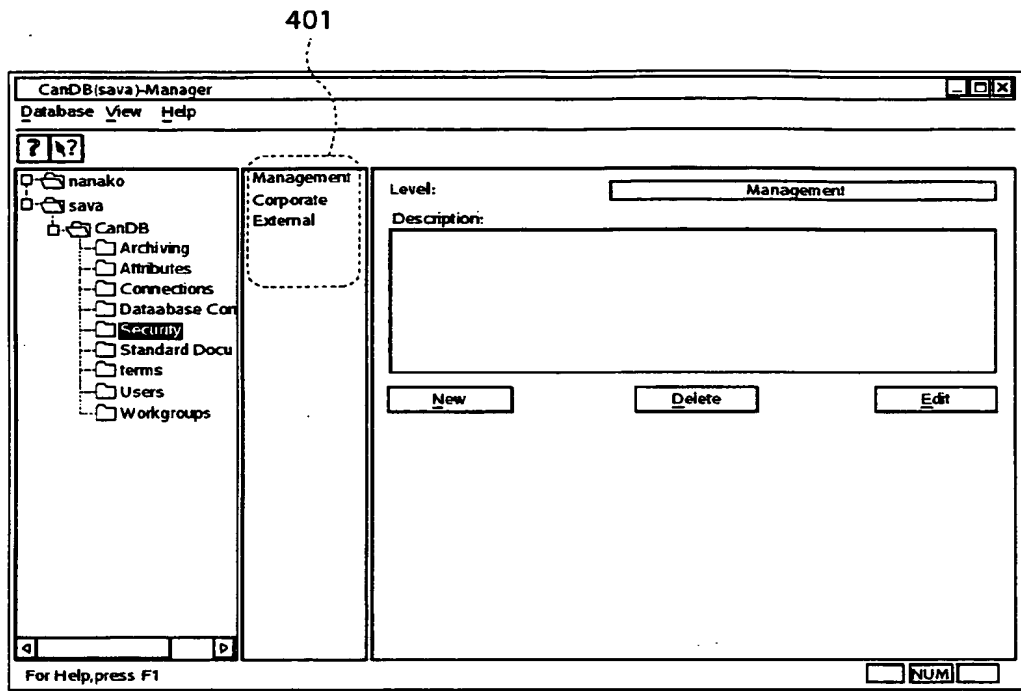
【図8】



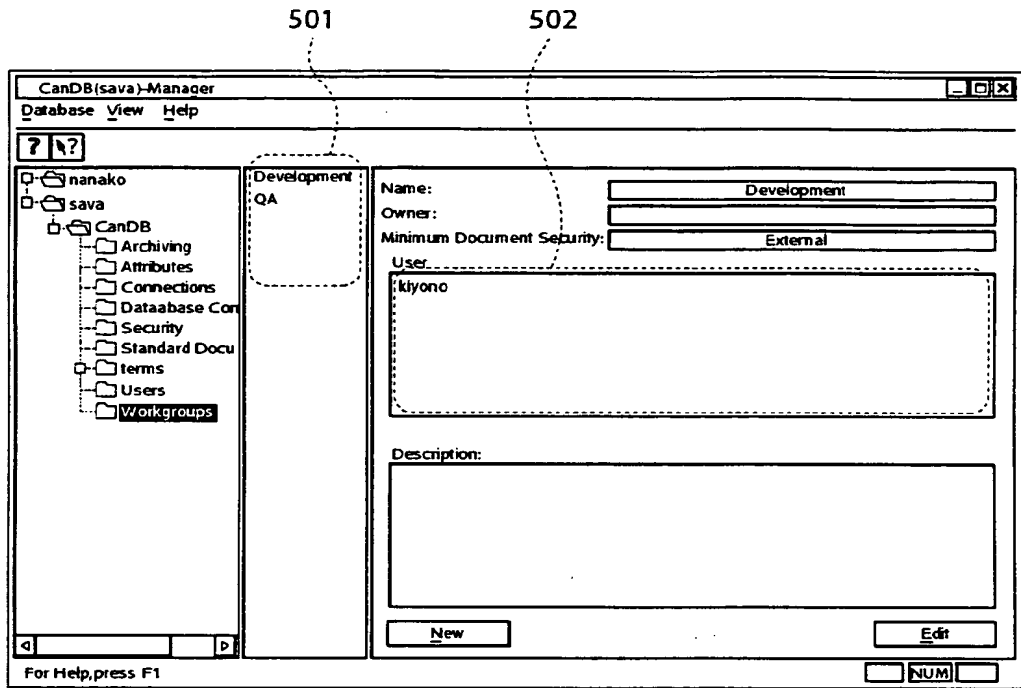
【図10】



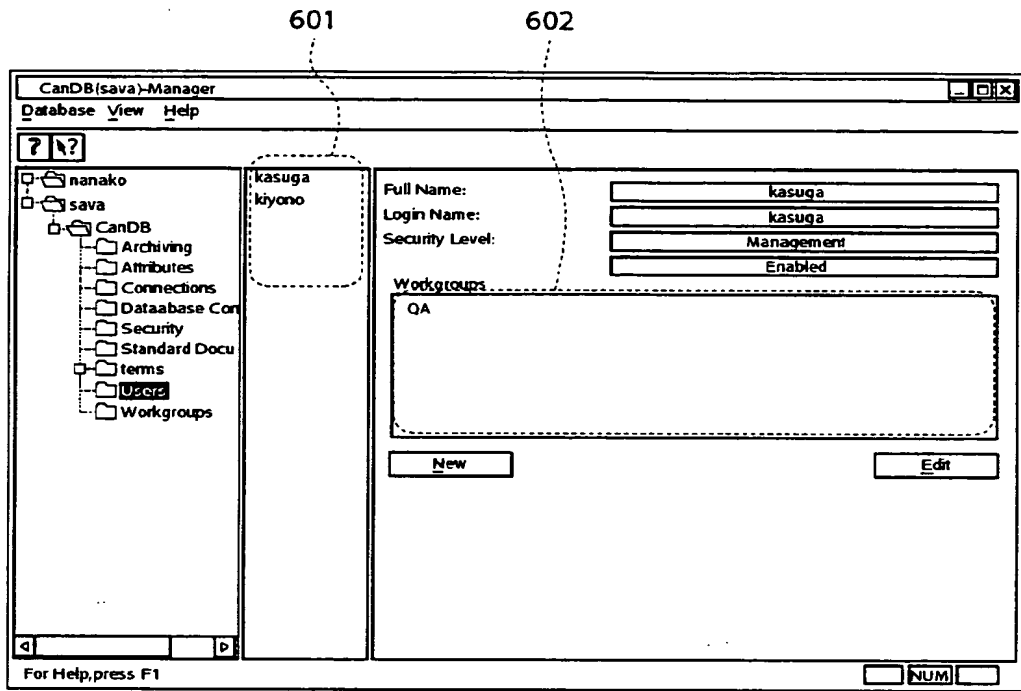
【図4】



【図5】




【図6】



【図7】

**DO Project Properties**

Attributes System Transactions Notes Version Links

 Budget1998.ppt

Version: 3

Creation: 19 November 1998

Checked In: 25 November 1998

Author: Mark

Owner: Andrew

Retention: Deactivated if not used for 12 months and purged from the archive after 10 years

**Security**

☐ Owner Only

☐ Group Only

☐ Security Level Only

☐ Group OR Security Level

☒ Group AND Security Level

Group: Development

Security Level: Management

OK Cancel Apply

701 702 703